(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 August 2002 (01.08.2002)

PCT

(10) International Publication Number
WO 02/060210 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/NO02/00035

(22) International Filing Date: 23 January 2002 (23.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20010427 24 January 2001 (24.01.2001) NO

(71) Applicant *(for all designated States except US)*: **TELENOR ASA** [NO/NO]; Snarøyveien 30, N-1331 FORNEBU (NO).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SANDBERG, Leif** [SE/SE]; Jäntens väg 14, S-132 35 Saltsjö-Bo (SE). **RØDBERG-LARSEN, Kjell** [NO/NO]; Myrveien 7, N-1406 Hebekk (NO).

(74) Agent: **OSLO PATENTKONTOR AS**; P.O. Box 7007 M, N-0306 Oslo (NO).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), DE (utility model), DK (utility model), DM, DZ, EC, EE (utility model), ES, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

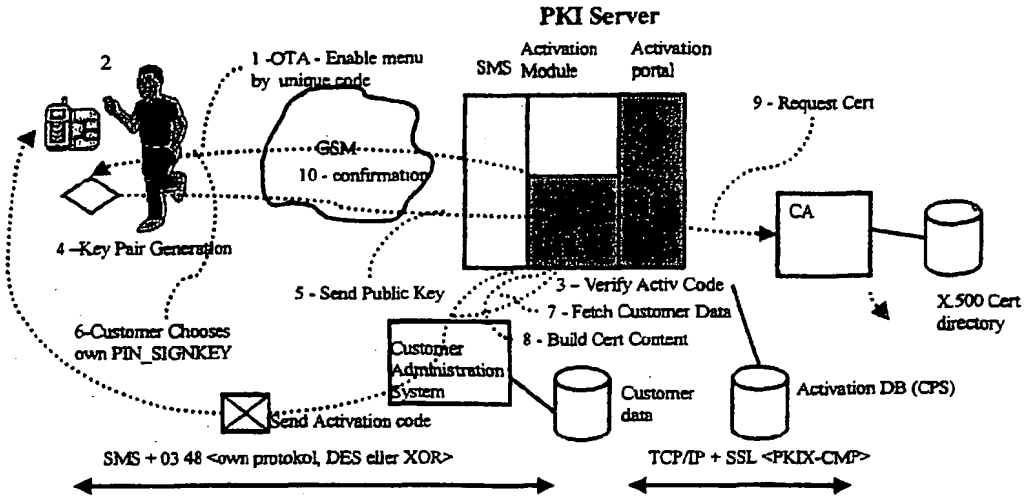
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES,

[Continued on next page]

(54) Title: METHOD FOR ENABLING PKI FUNCTIONS IN A SMART CARD



(57) Abstract: The present invention discloses a method for enabling at least a part of a Smart Card. According to a preferred embodiment of the present invention, a one time activation code is generated in a server at a telephone operator. The activation code is sent via registered mail to a user of a Smart Card, e.g. a SIM card in a GSM cellular phone. When the user enters the activation code into the cellular phone, the entry is transmitted to the server for verification. Upon successful verification, the server transmits an enabling command to the phone for thereby enabling the intended part of the SIM card. This may be enabling of PKI functionalities that until now have been hidden in the SIM card and thus unavailable for the user. The user may then choose his own signing PIN for authentication, encryption and transaction signing. In case of enabling PKI functions, all necessary generation of private and public keys and establishment of certifications are carried through when the activation code is verified.

WO 02/060210 A1

FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method for enabling PKI functions in a Smart Card

Field of the invention

The present invention is related to Smart Cards and communication network, in particular a mobile telephone system using a one time activation code for activating at least a part of a Smart Card, e.g. PKI (Public Key Infrastructure) function in a SIM (Subscriber Identity Module) card.

Background of the invention

PKI functions in a Smart Card, e.g. a SIM card localized in a GSM cellular phone, is normally protected by its own PIN code and PUK code (not the same as for the GSM part). The PIN code is normally a relatively short personal number which has to be entered to enable the card for use. The PUK code is normally a much longer number which has to be entered after tree times of incorrectly entry of the PIN code. This prevents unauthorized access to the Smart Card.

For security reasons the PUK code must be considerably longer than the PIN code. However, this emerges as a problem for the user because the code is difficult to remember. For most users it is necessary to store the PUK code e.g. on a piece of paper, and on rare occasions, when the PUK code is needed, it may probably be gone. Due to this, mobile telephone operators (or any other type of issuer) frequently have to replace the users Smart Card/ SIM. Because of security reasons, it is not a proper handling to reprint a PUK twice. This will imply extra cost and work to renew the subscription with a new PUK and a Smart Card as well.

The PUK code is a fixed code, thus requiring storage of the code locally in the Smart Card. An additional problem due to the fact that the PUK code is a fixed code, is that the

Smart Card is tied up to one user during its life time, and there is no possibility for changing the user for a certain subscription. This implies manufacturing and distribution of more Smart Card than necessary.

Summary of the invention

It is an object of the present invention to provide a method that eliminates the drawbacks described above. The features defined in the claims enclosed characterize this method.

More specifically, according to the present invention an activation code replacing the PUK code is generated centrally and will be send preferably by registered mail to the user of the Smart Card that may be a SIM card localized in a cellular phone. The verification of the activation code is carried through simply by comparing (e.g. in a server of a telephone operator) the user entered activation code with the previously mailed one, which also is stored in the telephone operators activation server. The activation code is a one time code, and replaces all the functions of the PUK code for the PKI function. Additionally it may be used to enable stored, but for the user previously hidden, functionalities in the Smart Card, e.g. PKI functionalities.

Brief description of the drawing

Fig. 1 is a view of the components and the data flow in an embodiment of the present invention.

Detailed description

The present invention will now be described in conjunction with an example embodiment referring to the above mentioned figure. However, the present invention is not limited to this particular embodiment, but may be used in other appli-

cations with various substitutions without departing from the scope of the invention as defined in the enclosed claims.

The example embodiment is based upon a mobile telephone network wherein the fixed PUK codes are replaced with one time activation codes. In addition to replacing the traditional functions of the PUK code, the activation code may also be used to enable PKI functionalities stored in the SIM cards of the subscribers.

To make use of PKI functionalities, a user must in advance be registered and registration data must be verified at an RA (Registration Authority). All relevant registration data must be available for the server generating activation codes, typically a server localized at a telephone operator.

After successful registration, the user may then be provided with a one time activation code which is generated in the server. This code will be used to authenticate the user towards the server after the registration and to initiate the key generation process into the Smart Card. The one time activation code will be provided to the user in a sealed envelope that is sent by post, e.g. as a registered letter to the home address of the user.

However, before the user may enter the activation code, a "SIM PKI menu" must be enabled. Thus, the PKI server transmits a - for the user's SIM card unique - code to the users phone to enable the "SIM PKI menu". This unique code should not be confused with the actual activation code described above. This "SIM PKI menu", have until now been resting invisibly in the SIM card not accessible to the user. The Activation Module in the PKI server will also fetch some unique parameters from the Card Production system, which also is stored in the particular SIM to be used as code for enable PKI menu in the SIM.

When the "SIM PKI menu" is enabled, the user enters the activation code in his/her handset to enroll to the service. The activation code is sent by SMS to the PKI Server. The user has 3 attempts to enter this code correctly.

The Activation Module verifies that the entered activation code corresponds to the one previously transmitted one. The Activation Module then transmits a "Generate PKI keys enabling command" back to the SIM, and the key generation application in the SIM will generate key pairs comprising private key and verification public key.

The verification public key (VPuK) is transmitted by SMS to the Activation Module, and the SMS is preferably encrypted according to GSM 03.48 for protection of sensitive information.

The user is then requested to choose a PIN_SIGNKEY, which is a personal self chosen signing key used for e.g. transaction signing, encryption and authentication.

In the case of successful verification, the Activation Portal connects to the CA to issue a valid certificate with the public key associated with the user. This certificate is at the same time sent to a certification directory.

A confirmation of successful certification is sent back to the user and the PKI menu will then be disabled in the SIM. The PKI functions in the SIM card are now enabled.

The present invention replaces the PUK code for the PKI part (not to be confused with that one for the GSM part), which is usually, for security reasons, stored in two separated parts, with a one time activation code thus saving memory space and administration.

In addition, the present invention introduces a higher degree of security as no PUK is being stored neither centrally at the operator, nor in the terminal or on a piece of paper for the user to remember.

The present invention enables generating keys in connection with use of PKI, thus allowing the user to choose the signing PIN for authentication and transaction signing himself.

A further advantage with the present invention is that SIM cards may be reused for the user or for a new user then the PKI certificate renewal date (within 2-3 years) since new PKI data will be generated in the Smart Card for each new activation code.

The above-described example of the present invention is for illustrative purposes only. Other implementations and variations may be utilized without departing from the scope of the invention as defined in the following claims.

Patent claims

1. Method for enabling at least a part of a Smart Card, said Smart Card associated to a terminal, said terminal connected to a communication network to which a server also is connected, said Smart Card accessible for a user of said terminal,
characterized in the following steps:

- generating an activation code in said server
- sending said activation code to said user
- adapting said terminal to prompt said user for his/her reading of said activation code
- on response to said user's entry of said reading of said activation code into said terminal, transmitting said entry to said server through said communication network
- on responds to receiving said entry, comparing said entry with said activation code
- if said entry and said activation code are equal, transmitting an enabling command to said terminal through said communication network
- upon receiving said activation code, enabling said at least a part of said Smart Card.

2. Method as defined in claim 1,
characterized in that said part of said Smart Card is PKI functions and said server is a PKI server.

3. Method as defined in claim 2, characterized in that the step of enabling further includes the following steps:

- generating a key pair including a private key and a public key
- requesting said user to choose and enter a signing, encryption and authentication PIN into said terminal
- transmitting said public key to said PKI server through said communication network
- from said PKI server, requesting a certificate for said user from a CA

4. Method as defined in claim 2 or 3, characterized in that said PKI functions is stored in said Smart Card, but hidden for the user until enabling.

5. Method as defined in any of the preceding claims, characterized in that the step of adapting includes transmitting a menu enabling code to said terminal from said server providing said terminal with a menu for said prompting of said user for said reading of said activation code.

6. Method as defined in any of the preceding claims, characterized in that said communication network is a GSM network, said terminal is a GSM mobile telephone, and said Smart Card is a SIM card.

7. Method as defined in claim 6, characterized in that said transmitting of said reading from said terminal to said server is carried through via an SMS.

8. Method as defined in claim 6 or 7, characterized in that said activation code completely replaces the PUK code used for PKI.

9. Method as defined in any of the preceding claims, characterized in that said activation code is sent to the user via registered mail.

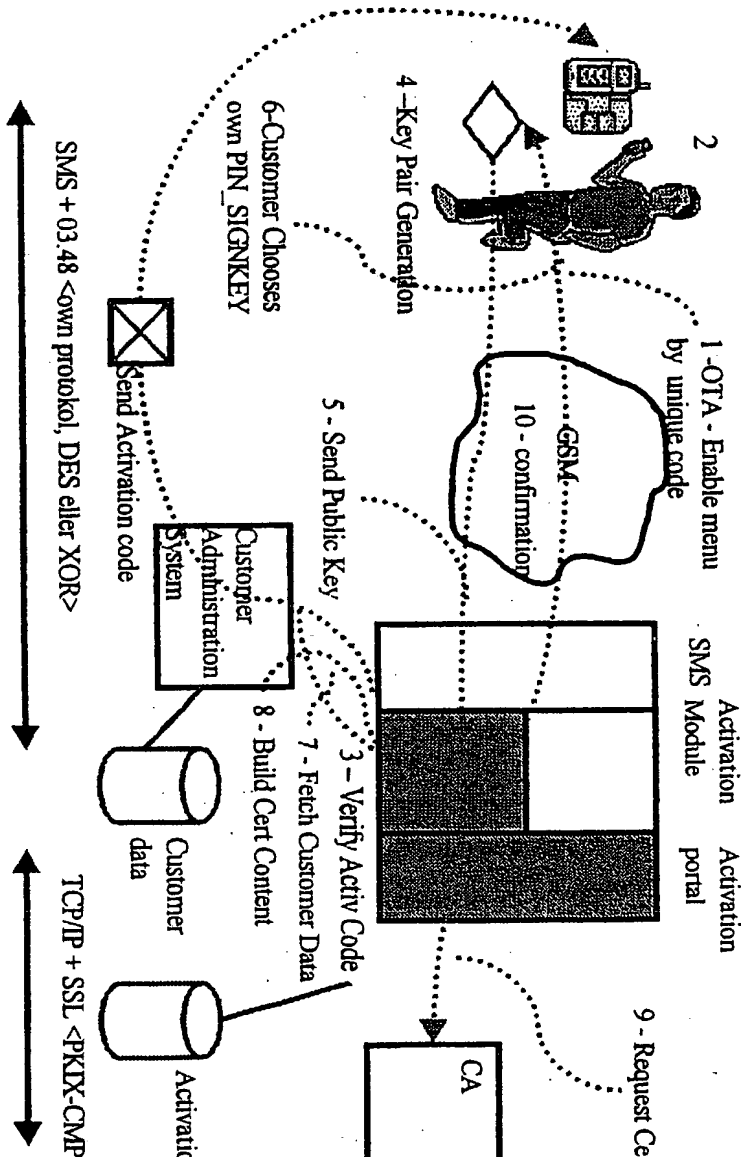

PKI Server
Activation portal
Activation SMS Module
CA
X.500 Cert directory
Activation DB (CPS)
Customer data
Customer Administration System
Send Activation code
2
1 -OTA - Enable menu by unique code
4 -Key Pair Generation
6-Customer Chooses own PIN_SIGNKEY
GSM
10 - confirmation
5 - Send Public Key
3 – Verify Activ Code
7 - Fetch Customer Data
8 - Build Cert Content
9 - Request Cert
SMS + 03.48 <own protokol, DES eller XOR>
TCP/IP + SSL <PKIX-CMP>

Fig. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 02/00035

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim N
A	WO 9833343 A1 (TELECOM FINLAND OY), 30 July 1998 (30.07.98), claims 11,12, abstract	1-9
A	US 5953422 A (M.F. ANGELO ET AL), 14 Sept 1999 (14.09.99), column 1 - column 3, abstract	1-9
A	DE 19820422 A1 (GIESECKE & DEVRIENT GMBH), 11 November 1999 (11.11.99), abstract	1-9
A	WO 0024218 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 27 April 2000 (27.04.00), abstract	1-9

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 May 2002	17 -05- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Thomas Tholin / MRo Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 02/00035

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 0054457 A1 (SONERA SMARTTRUST OY), 14 Sept 2000 (14.09.00), page 3 - page 6, abstract -- --------	1-9

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/05/02

International application No.
PCT/NO 02/00035

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9833343 A1	30/07/98	AU 736486 B	26/07/01
		AU 5865998 A	18/08/98
		CN 1244997 T	16/02/00
		EP 0965238 A	22/12/99
		FI 3204 U	16/12/97
		FI 104937 B	00/00/00
		FI 970339 A,V	28/07/98
		HU 0002794 A	28/12/00
		IL 131020 D	00/00/00
		JP 2001509333 T	10/07/01
		NZ 336833 A	24/11/00
		TR 9902365 T	00/00/00
US 5953422 A	14/09/99	EP 0851335 A	01/07/98
DE 19820422 A1	11/11/99	AU 3824199 A	23/11/99
		CN 1299497 T	13/06/01
		EP 1076887 A	21/02/01
		WO 9957689 A	11/11/99
WO 0024218 A1	27/04/00	AU 1422200 A	08/05/00
		CN 1326654 T	12/12/01
		DE 19983656 T	13/09/01
		SE 9803569 A	20/04/00
WO 0054457 A1	14/09/00	AU 3168800 A	28/09/00
		EP 1161813 A	12/12/01
		FI 4360 U	28/02/00
		FI 108813 B	00/00/00
		FI 990502 A,V	09/09/00

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 August 2002 (01.08.2002)

PCT

(10) International Publication Number
WO 02/060210 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/NO02/00035

(22) International Filing Date: 23 January 2002 (23.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20010427 24 January 2001 (24.01.2001) NO

(71) Applicant *(for all designated States except US)*: **TELENOR ASA** [NO/NO]; Snarøyveien 30, N-1331 FORNEBU (NO).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SANDBERG, Leif** [SE/SE]; Jäntens väg 14, S-132 35 Saltsjö-Bo (SE). **RØDBERG-LARSEN, Kjell** [NO/NO]; Myrveien 7, N-1406 Hebekk (NO).

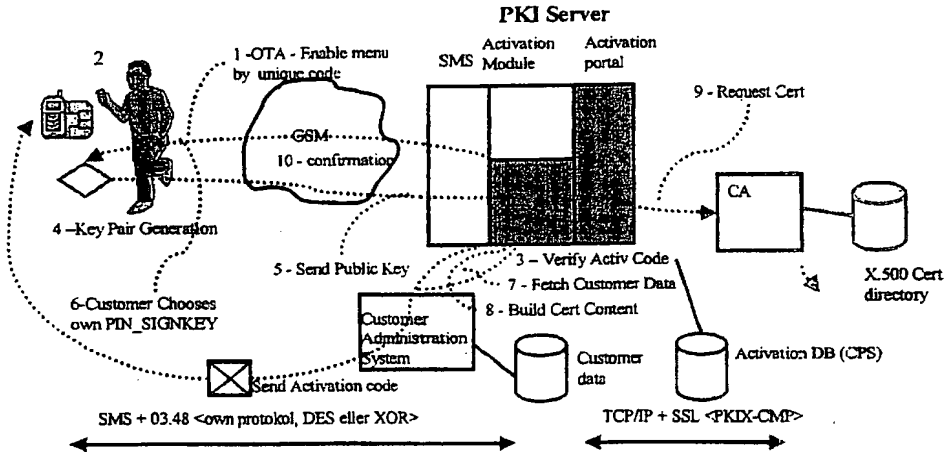
(74) Agent: **OSLO PATENTKONTOR AS**; P.O. Box 7007 M, N-0306 Oslo (NO).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR ENABLING PKI FUNCTIONS IN A SMART CARD



(57) Abstract: The present invention discloses a method for enabling at least a part of a Smart Card. According to a preferred embodiment of the present invention, a one time activation code is generated in a server at a telephone operator. The activation code is sent via registered mail to a user of a Smart Card, e.g. a SIM card in a GSM cellular phone. When the user enters the activation code into the cellular phone, the entry is transmitted to the server for verification. Upon successful verification, the server transmits an enabling command to the phone for thereby enabling the intended part of the SIM card. This may be enabling of PKI functionalities that until now have been hidden in the SIM card and thus unavailable for the user. The user may then choose his own signing PIN for authentication, encryption and transaction signing. In case of enabling PKI functions, all necessary generation of private and public keys and establishment of certifications are carried through when the activation code is verified.

WO 02/060210 A1

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

(48) Date of publication of this corrected version:
11 December 2003

(15) Information about Correction:
see PCT Gazette No. 50/2003 of 11 December 2003, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.